SMT Briefing: DfE Meeting digital and technology standards in schools and colleges

Introduction

The DfE has produced guidance on how to meet their digital and technology standards here: https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges. The standards set out in the DfE guidance are generic in nature and require considerable interpretation when developing a plan to meet them, or to see whether they are currently being met.

The NEN has developed a set of technical guides - https://nen.gov.uk/advice/standard-network-design/ - that supplement the DfE standards and can be used by technical staff to audit the current IT provision and provide a framework for future planning.

The purpose of this briefing note is to provide a distillation of the DfE documents for senior management. It is not intended to replace the DfE guides but to provide a high level overview as an aid to understanding. No specific recommendations are included here: these are available in the full DfE guidance or NEN technical guides.

Each individual DfE standard is defined then followed by five sections: importance, when to meet, how to meet, technical requirements, and dependencies. This overview will include the first three, but not the technical or dependencies sections as these will usually be handled by the technical staff.

Broadband internet standards for schools and colleges

The Standard

Schools and colleges should use a full fibre connection for their broadband service with a backup connection and appropriate security and safeguarding systems in place.

> **IMPORTANCE**: A full fibre connection provides the necessary capacity for the effective use of online learning tools and the opportunity to use cloud based services. With increasing use of online resources a backup connection should be in place to mitigate any connection failures. Staff and student safety is paramount so appropriate cyber security standards, tools, training, and policies should be in place.
> **WHEN**: A full fibre connection should be in place as soon as practicable with a backup connection implemented either at the same time or soon thereafter. Security and safeguarding systems should already be in place but may need updating.
> **HOW**: Investigate availability of full fibre in your locality at the appropriate speeds for your site and backup connection options. Security should be discussed with your IT support or supplier.

Cloud solution standards for schools and colleges

The Standard

Where possible cloud services should be preferred to locally hosted systems. Chosen cloud systems must follow data protection legislation, use identity and access management tools, work on a range of devices, be accessible when needed, and include appropriate backup provision.

IMPORTANCE: Using cloud solutions reduces the need for local servers which can reduce the costs of maintenance, energy, replacement, software licensing, etc. Cloud services may also improve cyber security. Many schools use a hybrid model, moving some services onto the cloud while retaining onsite servers for some tasks. Any solution must comply with data protection legislation.

To avoid the need for multiple logins and passwords when using more than one cloud solution a central ID and access management tool should be used. This provides a single account for each user and greatly simplifies user management when they join or leave.

Any solution must work with a wide range of different systems and be reliable.

A comprehensive backup regime is just as important for cloud based data as that stored locally. Retention policies vary between cloud providers so need to be assessed for suitability. Independent, third party backups may be required.

To reap the benefits of a cloud based solution both users and managers need to be trained in its use.

WHEN: You should meet these standards as soon as possible to realise the benefits and keep your data systems secure.

HOW: Before moving to a cloud solution it is important that the current system is carefully analysed so that you have a clear understanding of what software, devices and data are used. Consideration can then be given to what data needs to be moved to and from the cloud: this then leads on to assessing what servers could be replaced by cloud solutions.

Once this analysis has taken place your IT provider should be tasked with setting up a cloud solution that meets this standard and your own needs. You must seek assurance from any cloud provider, in consultation with your data protection officer, that data is being held, shared, and retained appropriately.

Your service provider should work with you to procure and set up an ID management system which works with your current cloud solutions and will work with future solutions including curriculum tools.

Before entering a cloud solutions agreement you need to understand how and when it will be accessed by users and run trials before committing to buy.

Working with your DPO and IT service provider, make sure you understand your cloud provider's backup processes and policies. In particular what is backed up, is it GDPR compliant, how long for, and how often?

Training in all aspects of using a chosen solution should be provided: from user training to managing the system.

Cyber security standards for schools and colleges

The Standard

All connected devices should be protected by an edge or software firewall, be correctly configured, and regularly updated. A record of each device's configuration should be kept and all changes logged.

User accounts should have the minimum access to perform their role and accounts with access to sensitive information should use multi-factor authentication.

Anti-malware software should be used to protect all network devices and all software must be appropriately licenced, patched with the latest updates, and checked before being installed on any network connected device.

The site's backup regime should ensure that there are at least three backup copies of important data on at least two separate devices one of which must be off-site.

Business Continuity and Disaster Recovery plans must be in place, regularly tested, and include contingencies for possible cyber attack. Any serious cyber attack must be reported and all staff trained in the basics of Cyber Security.

The site must comply with the Data Protection Act and undertake an Impact Assessment for personal data.

IMPORTANCE: Firewalls help prevent cyber attacks and make scanning for potential targets harder. Attackers scan for devices they can exploit so any available security settings should be configured: this is basic cyber security.

Attackers who gain physical access to important devices (servers, routers, etc.) can exploit them more easily so access should be restricted as far as possible. Documenting network devices help keep the network up-to-date and aids recovery.

By limiting the number of administrator accounts you also limit the potential for damage of any successful attack. Multi-factor authentication protects against accounts be compromised: this is especially important for accounts with access to sensitive or personal data.

Anti-virus and anti-malware software reduce the risk from many cyber attacks. Applications can introduce malware or viruses onto the network so must be checked before being installed: users should not be able to install software. Using unlicensed software is illegal, and there is no guarantee that an unlicensed copy is legitimate and may introduce malware or a virus into the system. Outdated or unpatched software may be vulnerable to a known exploit providing a potential attacker with a known target.

Backups are crucial for recovery from unforeseen events. Having a copy off site is important in case of a catastrophic failure like, for example, a flood or fire.

Being unprepared for a cyber attacked will make recovery harder and more expensive. Good preparation can mitigate the effects and speed up recovery.

Cyber attacks should be reported. They are crimes that need to be investigated so perpetrators can be found and counter-measures identified.

A data protection impact assessment is required by statute for personal data: it is designed to protect staff and students, the site's reputation and avoid legal liabilities.

Most cyber incidents are the result of common mistakes by staff. Training in basic cyber security helps avoid these mistakes and raises awareness of the risks of cyber attacks.

WHEN: All elements of this standard should already be being met on your network. If not, implementing them should be a priority.

HOW: Ask your provider to set up an edge firewall and configure the software firewall on local devices where possible. Agree a system for monitoring logs, documenting any changes and updating as cyber threats change.

Critical network devices should be kept in secure cabinets or a server rooms to limit physical access. Your IT provider should record and set network devices so that they meet these standings and document their configuration. A process for review and recording changes should also be agreed.

Your IT provider should set up users accounts that meet this standard: each new account should be documented and only those rights required by the account to perform its function should be granted to it. A system for creating, approving, and removing accounts should be in place. It is good practise to set up multi-factor authentication on all accounts with access to sensitive or personal data. Only specific accounts should be allowed to install software.

Your IT provider should provide, setup, and maintain anti-virus and anti-malware software on all appropriate devices.

Ask your IT service provider to make sure all devices and software are licensed, up-to-date and supported. Replace any that cannot be updated and have a process to manage updates and replacement as software becomes unsupported.

Your IT provider should set up an appropriate backup regime.

Make sure you have appropriate contingency plans in place in the event of a cyber security incident. It should be regularly tested so that the appropriate staff and clear about what to do. Any cyber attacks should be reported to Action Fraud and the DfE.

Access to data should be restricted in consultation with your IT service provider and the Data Protection Officer. This is to safeguard both staff and students as required by the General Data Protection Regulation (GDPR).

Staff who require access to your IT network must take basic cyber security training every year. The training should be part of the induction training for new staff.

Digital Accessibility standards

The Standard

Digital accessibility means making digital products, content and services accessible and usable for all. Everyone should be able to access the same information and use the same equipment. Communication should be accessible to all.

IMPORTANCE: Education sites should be easily accessible to everyone in society. Including digital accessibility in policies and strategies can help ensure that barriers are removed, lead to better choices, and meet legal requirements. 1 in 5 people have some form of disability: these need to be catered for using a range of software and hardware.

Communication is key in all teaching and learning: any concerns raised by staff or parents need to be addressed as a matter of urgency.

WHEN: These standards should be actively addressed whenever policies or strategies are reviewed, or when new devices are being purchased.

HOW: The accessibility of digital assets should be reviewed and included in policies and strategies: e.g. SEND and curriculum policies. Staff, students, and parents should be included in designing these policies. Staff should know how to configure a device's accessibility features and the use of software and hardware to support individual needs.

A member of the SMT should have responsibility for accessibility and work with others (IT Lead, SEND lead, etc.) to ensure that appropriate hardware and software is being used to support those with any special needs.

With web-based materials becoming so important in education they must be designed with accessibility in mind: they should follow accepted standards when choosing colours, fonts, etc., and allow the use of text-based browsers and text-to-voice readers. Alternative forms of communications (email attachments, SMS, etc.) should also be considered where appropriate.

Staff training is important so that all staff appreciate the issues and have confidence in using the tools available.

Digital Leadership and Governance standards

The Standard

Good digital governance and leadership identifies roles and responsibilities, and establishes processes to manage the digital technology. Registers of hardware and software should be established and updated as devices come and go. The digital aspect of the site should be included in the disaster recovery (DR) and business continuity (BC) plans, and a digital strategy should be developed and reviewed every year.

IMPORTANCE: Clearly defined roles help focus the digital strategy around the more general development plan. Without this there is a risk of short-termism and incompatible devices being bought. The IT lead should be a senior member of the SMT and be responsible for the strategic oversight of the IT systems and ensure that they support staff and students.

For a comprehensive understanding of the digital estate requires accurate registers of digital assets, software, contracts, licences, etc. This data forms the basis of effective and economic management.

Each site should have DR and BC plans: a key part of these will be the role digital technology plays. Plans should to be in place that define the actions that need to be taken in the event of either one being implemented.

Once the current system is understood a Digital Strategy can be written which allows decisions on IT purchases, etc. to be taken in a way that best meets the future needs of the site.

WHEN: An IT lead will need to be assigned before the digital Strategy is developed. The Registers should be updated continuously as soon as possible. If they do not exist then they should be created as part of an audit of the current digital estate.

You should already be meeting this standard as insurance companies may ask for DR and BC plans as part of a risk assessment.

HOW: The Principal, Headteacher should make the appointment: they need not be an expert but should have some technical expertise and an interest in IT would be advantageous. The IT lead will be responsible for creating (or causing to be created) the required registers and setting up processes to ensure their accuracy.

Both these plans need continual updating as the environment changes: it should be tested annually to identify and gaps that need to be addressed.

The IT lead will be responsible for the Digital Strategy's development in consultation with all stakeholders: heads of department, IT support, safeguarding lead, the governing body, etc.

Filtering and monitoring standards for schools and colleges

The Standard

You should have a filtering system which blocks inappropriate content without unduly impacting teaching and learning. It should be reviewed annually and strategies in place to ensure it is meeting the site's safeguarding needs. Specific roles and responsibilities for its management should be identified and assigned.

IMPORTANCE: Schools and colleges must provide a safe environment. Filtering and monitoring are important for safeguarding everyone by blocking access to harmful and inappropriate content online, and by monitoring online activity. Clear roles and responsibilities need to be in place with everyone working together to make informed decisions when issues arise.

The system(s) in place need to be regularly reviewed as technology develops to ensure performance to an acceptable level is maintained.

It needs to be understood that no filtering system is 100% effective at blocking harmful content: blocking too much (in an attempt to block all unwanted material) is also detrimental to teaching and learning.

Monitoring does not prevent online activity but allows incidents to be picked up quickly so that timely action can be taken by, for example, tweaking the filtering system to prevent future occurrences. A range of monitoring strategies are possible from physical overview to logging online activity and web access for later analysis.

WHEN: You should already be meeting this standard.

HOW: Governors and SMT have strategic responsibility in this area from defining the various roles, making sure the systems in place meet this standard, that regular reviews take place. The SMT will need support in the procurement and setting up of systems including processes for recording any issues.

How roles are defined and assigned will be specific to each site: not all will be able to provide suitable internal staff so some responsibilities may be assigned to external providers.

The SMT and safeguarding lead should conduct the reviews although the supplier may be required to offer support. The results should be recorded for future reference. System providers should be asked to provide systems training and support.

The designated safeguarding lead should take responsibility for acting on any issues flagged by the system and recording any actions taken.

Laptop, desktop and tablet standards

The Standard

All devices should meet the educational needs of both staff and pupils and support the site's digital technology strategy. Devices should be safe and secure: this will include physical security and network policies (e.g. using local firewalls and filtering software). All devices should meet or exceed the minimum requirements set out on the DfE website or NEN technical guide (see links above), should be energy efficient, and bought and disposed of sustainably.

IMPORTANCE: If devices do not meet the needs of staff and pupils then everything is harder: teaching days are lost, curriculum planning and delivery are compromised, administration is harder, maintenance and replacements costs are higher, etc.

Keeping devices safe and secure protects the users and network data while making it easier to deploy safeguarding policies consistently across the estate. It will also reduce the risks of theft and cyber attack.

Devices which do not meet the minimum requirements may not be able to run the newest software efficiently (or at all) which will have a detrimental effect on curriculum choices and pupils' and staff's perception of the devices they have to work with.

Energy efficient devices reduce costs and are less environmentally damaging. Sustainable purchase and disposal also helps reduce their environmental impact.

WHEN: Whenever new devices are purchased or existing ones reviewed, this standard must be the basis on which decisions are made to purchase, refurbish, or repurpose. Energy efficiency should be considered when investing in new equipment.

HOW: It is critical that the digital lead should work closely with IT support, and/or suppliers, to ensure that items bought are appropriate and meet the technical standards. The Digital Strategy should be used to asses the currently installed devices. Everything that is required to comply with the safety and security standard is covered in the Cyber security standard above.

Existing devices should be reviewed to see whether they meet this minimum standard and, if not, what to do with them: replace, refurbish, or repurpose. New devices must meet or exceed them.

The Digital Lead should review how all devices are used: are they turned off at night, are the power settings correct (e.g. automatically turning off the screen when not in use)? Do potential new devices have a low energy rating? If devices are disposed of then action must be taken to delete all the data on them.

Network cabling standards for schools and colleges

The Standard

Any copper cabling should be Cat 6A and optical fibre should be a minimum 16 core mult-mode OM4. These are technical standards that your supplier/installer will be aware of. New cabling should be installed and tested in line with the manufacturer's instructions, and warranty terms and conditions.

IMPORTANCE: Category 6A cable has higher capacity than older standards providing greater future-proofing as demand increases. Similarly, OM4 optical (fibre) cable provides high capacity over longer distances and should be used when connecting server rooms and switch cabinets together in the same building or between buildings.

The quality of cabling plays a critical role in making sure that data is transferred around the school: faulty or low specification cabling will negatively impact network performance.

WHEN: You should meet the standard when you need to replace old cabling/fibre or upgrade (part of) your network.

HOW: You should confirm with your supplier or in-house support that all cabling complies with British Standards 6701, 50173 and 50174 which cover the specification, installation, operation and maintenance of network cabling. Cables should be installed by manufacturer approved partners with the relevant accreditations who should also provide a detailed test report showing successful test results for all the installed network cables, based on the test limits defined in British Standards 50173.

Network switching standards for schools and colleges

The Standard

The network switches should provide fast, reliable, and secure wired and wireless connections with security features to prevent unauthorised access. Core switches should be connect to a UPS to mitigate power outages. The switch network should be managed via a central platform.

IMPORTANCE: You will have many users accessing the network at the same time: a high performance solutions allow data to be transferred quickly and securely, and performance will not degrade as more devices are added. A central management console will allow the network to be run efficiently by your IT support. Security is important to prevent unauthorised access to the switches and data stored on the network. A power outage in all or part of the network is very disruptive: critical network devices (switches, routers, etc) should be connected to at least one UPS to offer some mitigation of the effects.

WHEN: Take the opportunity to meet the standard when replacing any elements of you current solution that are failing, unsupported, underperforming, or scheduled for renewal.

HOW: Ask your IT support to ensure that critical switches and their connections have been identified and any actions needed to meet the standard are brought to the attention of the SMT.

Servers and storage standards for schools and colleges

The Standard

All servers and storage platforms should continue to work if any single component fails. They must also be secure and follow data protection legislation. They should be energy efficient, while meeting user needs, and be housed in a suitable physical environment.

IMPORTANCE: Servers and storage platforms must be designed to be secure and resilient to minimise the risk of systems or data being unavailable. System tools should provide alerts on failure. Insecure systems increase the risk of data loss and cyber attack leading to both financial and reputational damage.

To meet current data protection legislation IT systems should be "secure by design": this can be achieved by providing physical security, employing cyber security measures, and proper user management.

As these systems run continuously they use a lot of energy: buying energy efficient systems and setting them up correctly can save money.

As with all network devices (routers, switches, etc.) servers and storage platforms should be housed in secure locations reducing the risk of data loss and damage.

WHEN: You should already be meeting this standard to help safeguard, protect and secure your data and systems. It is also a requirement for meeting data protection legislation.

HOW: Cloud solutions reduce the need for local servers and the costs of managing them. Your service provider (internal or external) should set up and maintain your local servers and storage platforms to meet this standard.

Both existing systems and new should be assessed for their compliance with these standards and any changes required should be completed and noted. Compliance with these standards should be a required criterion for any new system and supplier assessed for their ability to meet them.

Energy efficiency should be considered when buying and setting up servers and storage platforms. Secure locations (server room(s) or secure cabinets) should be provided for all servers and other network devices.

Wireless network standards for schools and colleges

The Standard

Wireless installations should meet the latest standards as approved by the Wi-Fi Alliance and the signal should be fully functional internally throughout the site and externally where required. The wireless network should be managed centrally from a suitable software platform including security measures preventing unauthorised access to the network.

IMPORTANCE: Your site will have a high number of users accessing the network at the same time. A high-performance solution is needed so that the connection does not slow as more devices connect. A good wireless connection relies on signal strength, so it’s important to make sure the signal is strong everywhere mobile devices are to be used.

A wireless network is made up of multiple wireless access points (WAPs): a central management solution allows it to be monitored and configured easily.

The network should prevent access by unauthorised users. A wireless network without adequate security may allow unauthorised access: this could lead to data theft, misuse, or loss of access to sensitive data with possibly significant disruption and cost.

WHEN: You should meet the standard when you need to upgrade an underperforming or unsupported solution, or following a scheduled maintenance or configuration review.

HOW: WAPs should be installed across the site ensuring adequate coverage. You should ask your supplier or in-house support team to provide a wireless solution that uses the Wi-Fi 6 standard and provide a central management tool that can be used to configure the WAPs, monitor performance and provide alerts in the event of a failure. It should also be able to deliver security updates automatically as soon as they are available. Manual checks should also be undertaken.